and before they result in even more widespread abuses.

By Mr. DOMENICI:

S. 3420. A bill to amend the Emergency Petroleum Allocation Act of 1973 to authorize and require the President of the United States to allocate asphalt and asphalt derivatives, and for other purposes. Referred to the Committee on Interior and Insular Affairs.

Mr. DOMENICI. Mr. President, I send to the desk for appropriate reference, a bill to amend the Emergency Petroleum Allocation Act of 1973 to authorize and require the President of the United States to allocate asphalt and asphalt derivatives. The need for this legislation has been brought to my attention by construction company owners in New Mexico who are experiencing difficulty in obtaining asphalt used for roofing construction, paving highways, streets, and airport runways.

I received a letter from a contractor who was low bidder on a job, and before the contract was awarded, he was advised by the oil company that the price on asphalt had risen $5 per ton. There was no price escalating clause provided by the bid proposal. The contractor was further advised that the price to be charged would be that in effect on date of delivery of each shipment. This contractor was bound by the required bid bond and had no choice but to proceed.

Other contractors are disturbed by the fact that the supplier stipulates that delivery is contingent upon the availability of the material, with no guarantee or assurance that it will be furnished.

Mr. President, this type of situation is unhealthy for the construction industry as well as for the agencies who request bids, due to the uncertainty of the matter. I believe that if my legislation is enacted, it will help to alleviate this problem.

ADDITIONAL COSPONSORS OF BILLS AND JOINT RESOLUTIONS

S. 411

At the request of Mr. McGEE, the Senator from California (Mr. TUNNEY), the Senator from Tennessee (Mr. BROCK), the Senator from Iowa (Mr. HUGHES), and the Senator from South Dakota (Mr. McGOVERN) were added as cosponsors of S. 411, to amend title 39, United States Code, relating to the Postal Service, and for other purposes.

S. 2363

At the request of Mr. CRANSTON, the Senator from Wyoming (Mr. HANSEN) and the Senator from South Carolina (Mr. THURMOND) were added as cosponsors of S. 2363, a bill to amend chapter 39, of title 38, United States Code, relating to automobiles and adaptive equipment for certain disabled veterans and members of the Armed Forces.

S. 2488

At the request of Mr. KENNEDY, the Senator from Ohio (Mr. METZENBAUM) was added as a cosponsor of S. 2488, to extend title VII of the Older Americans Act of 1954, the nutrition for the elderly program.

S. 3168, S. 3199, AND S. 3170

At the request of Mr. GRIFFIN, for Mr. TOWER, the Senator from Minnesota (Mr. HUMPHREY) was added as a cosponsor of S. 3168, to amend title II of the Social Security Act to permit the payment of benefits to a married couple on their combined earnings record; S. 3169; to amend title II of the Social Security Act to provide that an insured individual otherwise qualified may retire and receive full old-age insurance benefits, at any time after attaining age 60, if he has been forced to retire at that age by a Federal law, regulation or order; and S. 3170, to amend title II of the Social Security Act to provide that any individual who has 40 quarters of coverage, whenever acquired, will be insured for disability benefits thereunder.

S. 3238

At the request of Mr. BENTSEN, the Senator from Tennessee (Mr. BROCK) was added as a cosponsor of S. 3238, the Taxpayer Privacy Act.

S. 3343

At the request of Mr. WEICKER, the Senator from Rhode Island (Mr. PELL), and the Senator from New Jersey (Mr. WILLIAMS) were added as cosponsors of S. 3343, to designate a national network of essential rail lines; to require minimum standards of maintenance on rail lines; to provide Federal financial aid for rail rehabilitation; to establish rights of access by rail carriers to rail lines and facilities, and for other purposes.

S. 3344

At the request of Mr. KENNEDY, the Senator from Rhode Island (Mr. PELL), the Senator from Missouri (Mr. EAGLETON), the Senator from California (Mr. CRANSTON) and the Senator from Minnesota (Mr. MONDALE) were added as cosponsors of S. 3344, a bill to authorize appropriations for activities of the National Science Foundation, and for other purposes.

S. 3371

At the request of Mr. EASTLAND, the Senator from South Dakota (Mr. McGOVERN) was added as a cosponsor of S. 3371, a bill to amend the Forest Pest Control Act of June 25, 1947.

S. 3378

At the request of Mr. ROBERT C. BYRD (for Mr. RANDOLPH), the Senator from Delaware (Mr. BIDEN) and the Senator from Minnesota (Mr. HUMPHREY) were added as cosponsors of S. 3378, the Developmentally Disabled Assistance and Bill of Rights Act.

SENATE JOINT RESOLUTION 203

At the request of Mr. ROTH, the Senator from Hawaii (Mr. INOUYE), the Senator from Ohio (Mr. METZENBAUM), and the Senator from New Mexico (Mr. DOMENICI) were added as cosponsors of Senate Joint Resolution 203, to authorize the President to issue a proclamation designating the month of May 1974 as "National Arthritis Month."

SENATE CONCURRENT RESOLUTION 83—SUBMISSION OF A CONCURRENT RESOLUTION RELATING TO THE SURGEON GENERAL'S REPORT

(Referred to the Committee on Rules and Administration.)

Mr. MAGNUSON (for himself and Mr. COTTON) submitted the following concurrent resolution:

SENATE CONCURRENT RESOLUTION 83

Resolved by the Senate (the House of Representatives concurring), that there be printed for the use of the Senate Committee on Commerce 1,000 additional copies of its hearings of the 92d Congress, second session, entitled "Surgeon General's Report by the Scientific Advisory Committee on Television and Social Behavior."

DEPARTMENT OF DEFENSE SUPPLEMENTAL APPROPRIATION AUTHORIZATION ACT—AMENDMENT

AMENDMENT NO. 1238

(Ordered to be printed and to lie on the table.)

Mr. KENNEDY. Mr. President, the amendment I am introducing to the Department of Defense supplemental appropriations authorization for 1974 (S. 2999), has three simple objectives.

First, it prohibits on the date of enactment any further transfer of funds for the Military Assistance Service Fund—MASF—for South Vietnam beyond those already obligated.

Second, the amendment reaffirms the decision of the Congress that the Pentagon must not spend one penny over the ceiling established for this fiscal year—$1.126 billion—for military aid to South Vietnam, notwithstanding the Armed Services Committee's finding that the Department of Defense wrongly charged $266 million to this year's ceiling.

Finally, Mr. President, the amendment puts the Pentagon on notice that the Congress is tired of the practice of shipping guns and ammunition now, and paying for them later. The amendment, in effect, supports the important recommendation of the Armed Service Committee that the Department must put its bookkeeping on military aid to South Vietnam in order, and that all military supplies delivered to Saigon during 1 fiscal year must be charged to that year's ceiling.

Mr. President, I ask unanimous con-

(1) any actual damages sustained by an individual;

(2) punitive damages where appropriate;

(3) in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

The United States consents to be sued under this section without limitation on the amount in controversy.

JURISDICTION OF DISTRICT COURTS

SEC. 305. The district courts of the United States have jurisdiction to enforce any subpena or order issued by the Federal Privacy Board under sections 102 or 103, respectively, of this Act.

RIGHT OF ACTION

SEC. 306. (a) Any individual who is denied access to information required to be disclosed under the provisions of this Act is entitled to judicial review of the grounds for such denial.

(b) The district courts of the United States have jurisdiction to hear and determine civil actions brought under subsection (a) of this section.

EFFECTIVE DATE

SEC. 307. This Act shall take effect one year after the date of its enactment.

AUTHORIZATION OF APPROPRIATIONS

SEC. 308. There are authorized to be appropriated such sums as may be necessary to carry out the provisions of this Act.

Mr. PERCY. Mr. President, I am pleased to join our distinguished chairman, Senator ERVIN, in introducing a bill to establish a Federal Privacy Board to oversee the gathering and safeguard the disclosure of information concerning individuals. The bill will provide standards for personal information maintenance and management systems in all Federal agencies, State and local governments, and other organizations.

The collection of information about individuals by Federal agencies, State and local governments, and private organizations, has vastly increased the potential for abuse of the individual's right to privacy. And the potential for abuse is magnified almost beyond imagination by the automatic data processing techniques that are now readily available to many organizations.

In the wake of this cybernetic revolution, many social scientists are turning to a new definition of privacy—a definition expressed by Professor Alan Westin in his book, "Privacy and Freedom." Privacy, according to Dr. Westin, is "the claim of individuals, groups, or institutions to determine for themselves, when, how, and to what extent information about themselves is communicated to others." Given this new attitude toward personal privacy, it is quite easy to understand the growing alarm with which many Americans regard the unchecked practices of Government and private organizations in collecting, maintaining, and disseminating personal information.

GOVERNMENT RECORDKEEPING AND THE RIGHT TO PRIVACY

Collection of data about people is of course not a new phenomenon. The Federal Government has been collecting immense amounts of very sensitive information on individuals for decades—income tax, social security, and the census come to mind immediately. This appetite for information has grown simultaneously with our increased reliance on the Federal Government for our health, safety and well-being. Americans have in general participated in this information-gathering process with good nature. Until rather recently there has been no widespread perception that the traditional recordkeeping practices of the Government posed any real threat to personal privacy.

However, the continuing application of highly sophisticated and centralized information technology to collecting and using personal data has drastically changed the implications of Government and private record-gathering for personal privacy. The advent of computers has increased by geometric proportions the amount of information the Government can collect about us. Prof. Arthur Miller of the Harvard Law School suggests that it will soon be feasible to store a 20-page dossier on every single American on a single piece of computer tape less than 5,000 feet long.

And we must be aware that, along with this increased capacity to gather and hold information, computerization has correspondingly enlarged the Government's ability quickly and automatically to disseminate personal information to other Federal agencies, State or local governments, and private organizations.

INFORMATION TECHNOLOGY AND THE PRIVATE SECTOR

The information-gathering impulse of the Federal Government is mirrored by similar developments in the private sector. Credit agencies with their consumer files have proliferated in recent years; educational institutions are beginning the process of computerizing student records; hospitals and medical centers are finding computers the answer to much of their recordkeeping difficulties. When such information is stored on tape, it is easily transferred from one user to another. The individual usually has no knowledge of the transfer, and no ability to correct information about himself that could ruin his chances for a new job, prevent his acceptance to college, or be taken as cause for investigation by a law enforcement agency—information that by its stigma could affect the entire course of his life.

Individuals are finding it increasingly difficult to make such simple transactions as obtain a loan, open a charge account, obtain a driver's license, or register to vote without divulging their social security number. The result is that the individual social security number becomes the code under which data about the person can be grouped, stored, and transferred from one agency to another. The effects of computer technology reach all of us in indirect, hidden ways that we may never know or even be able to know, as well as in obvious ways.

We have reached the time when we must assert control over runaway technology, and protect the individuals' "freedom of privacy" from haphazard abuse. We must shape our tools, lest they shape us.

PRIVACY AND THE 93D CONGRESS

Despite the multitude of bills and resolutions introduced relating to personal privacy, there has to date been no bill introduced in the Senate which deals with the issue of privacy on a comprehensive basis. Most bills now pending are directed to only one aspect of the privacy question: pending bills range from banning the disclosure of social security numbers to prohibiting financial institutions from disseminating information on their customers to Government agencies. Hearings have been held on restricting existing practices of criminal information systems, banning political surveillance by the Army, and controlling illicit uses of wiretapping. With all this isolated activity taking place, it is difficult to understand and appreciate the major theme which runs through these seemingly disparate pieces of legislation.

The common thread is the individual's right to control how, when, and to what extent information about himself is communicated to others. Until today no legislation has attempted a comprehensive response to this problem. This bill is a companion measure to one introduced in the House under the inspired leadership of Congressman BARRY GOLDWATER JR. and Congressman EDWARD KOCH.

This bill is the first major effort to respond to the threat to personal privacy on a comprehensive basis. It is directed toward controlling the threat to privacy at three important and distinct stages: collection, storage, and dissemination of information on private citizens by Federal agencies, State and local governments, and by private organizations.

The bill establishes a Federal Privacy Board which will serve as an oversight agency, establishing and enforcing standard rules and regulations designed to protect individual privacy throughout all public and private information systems, with the exception of those that relate to national defense, criminal investigations, or information gathered by the media. The Federal Privacy Board will have the authority it needs to exercise centralized control over information systems through subpena power, the right to hold open hearings, and the right to recommend both criminal and civil sanctions against offenders. The bill will establish the procedures under which individuals may get direct access to information about them, and provide a ready means for challenging and correcting that information.

The protection of personal privacy is no easy task. It will require foresight and the ability to forecast the possible trends in information technology and information policies of our Government and of the private sector before they actually take their toll in widespread invasions of personal privacy. The Congress must act before these new systems are developed

information including all classes of users and the organizational relationships among them;

(H) the procedures whereby an individual may (i) be informed if he is the subject of information in the system, (ii) gain access to such information, and (iii) contest the accuracy, completeness, timeliness, pertinence, and the necessity for retention of such information;

(I) the procedures whereby an individual or group can gain access to the information system used for statistical reporting or research in order to subject them to independent analysis; and

(J) the business address and telephone number of the person immediately responsible for the system.

(d) Any such organization maintaining personal information shall—

(1) inform any individual asked to supply personal information whether such individual is required by law, or may refuse, to supply the information requested, and also of any specific consequences which are known to the organization of providing or not providing such information;

(2) request permission of a data subject to disseminate part or all of such information to another organization or system not having regular access authority, and indicate the use for which such information is intended, and the specific consequences for the individual, which are known to the organization, of providing or not providing such permission;

(3) upon request and proper identification of any individual who is a data subject, grant such individual the right to inspect, in a form comprehensible to such individual—

(A) all personal information about that individual except that, in the case of medical information, such information shall, upon written authorization, be given to a physician designated by the individual;

(B) the nature of the sources of the information, and

(C) the recipients of personal information about such individual including the identity of all persons and organizations involved and their relationship to the system when not having regular acces authority;

(4) at a minimum, make disclosures which are required by this Act to individuals who are data subjects—

(A) during normal business hours;

(B) in person, if the data subject appears in person and furnishes proper identification, or by mail, if the data subject has made a written request, with proper identification, at reasonable standard charges for document search and duplication; and

(C) permit the data subject to be accompanied by one person of his choosing, who must furnish reasonable identification, except that an organization may require the data subject to furnish a written statement granting permission to the organization to discuss that individual's file in such person's presence;

(5) upon receipt of notice from any individual who is a data subject, that such individual wishes to challenge, correct, or explain information about him in such system—

(A) investigate and record the current status of such personal information;

(B) purge any such information that is found to be incomplete, inaccurate, not pertinent, not timely nor necessary to be retained, or can no longer be verified;

(C) accept and include in the record of such information, if the investigation does not resolve the dispute, any statement (not more than two hundred words in length) provided by such individual setting forth his position on such disputed information;

(D) in any subsequent dissemination or use of disputed information, clearly note that such information is disputed and supply the statement of such individual together with such information;

(E) make clear and conspicuous disclosure to such individual of his right to make a request under this paragraph;

(F) at the request of such individual, following any correction or purging of personal information, furnish to past recipients of such information notification that the item has been purged or corrected; and

(G) in the case of a failure to resolve a dispute, advise such individual of his right to request the assistance of the Federal Privacy Board.

(e) Each such organization maintaining a personal information system on the date of the enactment of this Act shall notify by mail each data subject of the fact not later than two years following the date of enactment of this Act, at the last known address of the subject. Such notice shall—

(1) describe the type of information held in such system or systems, expected uses allowed or contemplated; and

(2) provide the name and full address of the place where the data subject may obtain personal information pertaining to him, and in the system.

(f) Data subjects of archival-type inactive files, records, or reports shall be notified by mail of the reactivation, accessing, or reaccessing of such files, records, or reports not later than six months after the date of the enactment of this Act.

(g) The requirements of subsections (a) (3) and (4) and subsections (c) and (d) (1) and 2) of this section shall not apply to any organization that (1) maintains an information system that disseminates statistical reports or research findings based on personal information drawn from the system, or from systems of other organizations, (2) purges the names, personal numbers, or other identifying particulars of individuals, and (3) certifies to the Federal Privacy Board that no inferences may be drawn about any individual.

EXEMPTIONS

SEC. 202. The provisions of this title shall not apply to personal information systems—

(1) to the extent that information in such systems is maintained by a Federal agency, and the head of that agency determines that the release of the information would seriously damage national defense;

(2) which are part of active criminal investigatory files compiled by Federal, State, or local law enforcement organizations, except where such files have been maintained for a period longer than is necessary to commence criminal prosecution; or

(3) maintained by the press and news media, except information relating to employees of such organizations.

USE OF SOCIAL SECURITY NUMBER

SEC. 203. It shall be unlawful for any organization to require an individual to disclose or furnish his social security account number, for any purpose in connection with any business transaction or commercial or other activity, or to refuse to extend credit or make a loan or to enter into any other business transaction or commercial relationship with an individual (except to the extent specifically necessary for the conduct or administration of the old-age, survivors, and disability insurance program established under title II of the Social Security Act) in whole or in part because such individual does not disclose or furnish such number, unless the disclosure or furnishing of such number is specifically required by law.

TITLE III—MISCELLANEOUS

DEFINITIONS

SEC. 301. As used in this Act—

(1) the term "Board" means the Federal Privacy Board;

(2) the term "information system" means the total components and operations of a recordkeeping process, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars;

(3) the term "personal information" means all information that describes, locates or indexes anything about an individual including his education, financial transactions, medical history, criminal, or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution;

(4) the term "data subject" means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system;

(5) the term "disseminate" means to release, transfer, or otherwise communicate information orally, in writing, or by electronic means;

(6) the term "organization" means any Federal agency; the government of the District of Columbia; any authority of any State, local government, or other jurisdiction; any public or private entity engaged in business for profit, as relates to that business;

(7) the term "purge" means to obliterate information completely from the transient, permanent, or archival records of an organization; and

(8) the term "Federal agency" means any department, agency, instrumentality, or establishment in the executive branch of the Government of the United States and includes any officer or employee thereof.

TRADE SECRETS

SEC. 302. In connection with any dispute over the application of any provision of this Act, no organization shall reveal any personal information or any professional, proprietary, or business secrets; except as is required under this Act. All disclosures so required shall be regarded as confidential by those to whom they are made.

CRIMINAL PENALTY

SEC. 303. Any organization or responsible officer of an organization who willfully—

(1) keeps an information system without having notified the Federal Privacy Board; or

(2) issues personal information in violation of this Act;

shall be fined not more than $10,000 in each instance or imprisoned not more than five years, or both.

CIVIL REMEDIES

SEC. 304. (a) The Attorney General of the United States, on the advice of the Federal Privacy Board, or any aggrieved person, may bring an action in the appropriate United States district court against any person who has engaged, is engaged, or is about to engage in any acts or practices in violation of the provisions of this Act or rules of the Federal Privacy Board, to enjoin such acts or practices.

(b) Any person who violates the provisions of this Act, or any rule, regulation, or order issued thereunder, shall be liable to any person aggrieved thereby in an amount equal to the sum of—

TITLE I—FEDERAL PRIVACY BOARD

ESTABLISHMENT OF BOARD

SEC. 101. (a) There is established in the executive branch of the Government the Federal Privacy Board which shall be composed of five members who shall be appointed by the President by and with the advice and consent of the Senate from among members of the public at large who are not officers or employees of the United States. Not more than three of the members of the Board shall be adherents of the same political party.

(b) The Chairman of the Board shall be elected by the members of the Board every two years.

(c) Each member of the Board shall be compensated at the rate provided for GS–18 under section 5332 of title 5 of the United States Code.

(d) Members of the Board shall be appointed for a term of three years. No member may serve more than two terms.

(e) Vacancies in the membership of the Board shall be filled in the same manner in which the original appointment was made.

(f) Vacancies in the membership of the Board, as long as there are three members in office, shall not impair the power of the Board to execute the functions of the Board. Three members of the Board shall constitute a quorum for the transaction of business.

(g) Members of the Board shall not engage in any other employment during their tenure as members of the Board.

FUNCTIONS OF THE BOARD

SEC. 102. The Board shall—

(1) publish an annual Data Base Directory of the United States containing the name and characteristics of each personal information system;

(2) consult with the heads of appropriate departments, agencies, and instrumentalities of the Government in accordance with section 103(5) of this Act;

(3) make rules to assure compliance with title II of this Act; and

(4) perform or cause to be performed such research activities as may become necessary to implement title II of this Act, and to assist organizations in complying with the requirements of such title.

POWERS OF THE BOARD

SEC. 103. (a) The Board is authorized—

(1) to be granted admission at reasonable hours to premises where any information system is kept or where computers or equipment or recordings for automatic data processing are kept, and may, by subpena, compel the production of documents relating to such information system or such processing as is necessary to carry out its functions, except that the production of personal information shall not be compelled without the prior consent of the data subject to which it pertains;

(2) upon the determination of a violation of any provision of this Act or regulation promulgated under this Act, to, after opportunity for a hearing, order the organization violating such provision to cease and desist such violation;

(3) to delegate its authority under this title, with respect to information systems within a State or the District of Columbia, to such State or District, during such period of time as the Board remains satisfied that the authority established by such State or District to carry out the requirements of this Act in such State is satisfactorily enforcing those provisions;

(4) to conduct open, public hearings on all petitions for exceptions or exemptions from provisions, application, or jurisdiction of this Act, except that the Board shall not have authority to make such exceptions or exemptions but shall submit appropriate reports and recommendations to Congress; and

(5) to the fullest extent practicable, to consult with the heads of appropriate departments, agencies, and instrumentalities of the Government in carrying out the functions of the Board under this Act.

(b) The Board may procure such temporary and intermittent services to the same extent as is authorized by section 3109 of title 5, United States Code, but at rates not to exceed $100 a day for individuals.

REPORTS

SEC. 104. The Board shall report, annually, on its activities to the Congress and the President.

TITLE II—STANDARDS AND MANAGEMENT SYSTEMS FOR HANDLING INFORMATION RELATING TO INDIVIDUALS

SAFEGUARD REQUIREMENTS FOR ADMINISTRATIVE, STATISTICAL-REPORTING AND RESEARCH PURPOSES

SEC. 201. (a) Any Federal agency, State or local government, or any other organization maintaining an information system that includes personal information shall—

(1) collect, maintain, use, and disseminate only personal information necessary to accomplish a proper purpose of the organization;

(2) collect information to the greatest extent possible from the data subject directly;

(3) establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;

(4) maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject;

(5) make no dissemination to another system without (A) specifying requirements for security and the use of information exclusively for the purposes set forth in the notice required under subsection (c) including limitations on access thereto, and (B) determining that the conditions of transfer provide substantial assurance that those requirements and limitations will be observed;

(6) transfer no personal information beyond the jurisdiction of the United States without specific authorization from the data subject or pursuant to a treaty or executive agreement in force guaranteeing that any foreign government or organization receiving personal information will comply with the applicable provisions of this Act with respect to such information;

(7) afford any data subject of a foreign nationality, whether residing in the United States or not, the same rights under this Act as are afforded to citizens of the United States;

(8) maintain a list of all persons having regular access to personal information in the information system;

(9) maintain a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority;

(10) take affirmative action to establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the system, or the collection or use of any personal information contained therein, of the requirements of this Act, including any rules and procedures adopted pursuant to this Act and the penalties for noncompliance;

(11) establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security;

(12) comply with the written request of any individual who receives a communication in the mails, over the telephone, or in person from a commercial organization, who believes that the name or address or both, of such individual is available because of its inclusion on a mailing list, to remove such name or address, or both, from such list; and

(13) collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects which is maintained, used or disseminated in or by any information system operated by any governmental agency, unless authorized by law.

(b)(1) Any such organization maintaining an information system that disseminates statistical reports or research findings based on personal information drawn from the system, or from systems of other organizations, shall—

(A) make available to any data subject or group (without revealing trade secrets) methodology and materials necessary to validate statistical analyses, and

(B) make no materials available for independent analysis without guarantees that no personal information will be used in a way that might prejudice judgments about any data subject.

(2) No Federal agency shall—

(A) require any individual to disclose for statistical purposes any personal information unless such disclosure is required by law, and such individual is informed of such requirement;

(B) request any individual to voluntarily disclose personal information unless such request is specifically authorized by law, and the individual is advised that such disclosure is voluntary;

(C) make available to any person, other than an authorized officer or employee of a Federal agency, any statistical study or reports or other compilation of information derived by mechanical or electronical means from any file containing personal information, or any manual or computer material relating thereto, except those prepared, published, and made available for general public use; or

(D) publish statistics of taxpayer income classified, in whole or in part, on the basis of a coding system for the delivery of mail.

(c) Any such organization maintaining or proposing to establish an information system for personal information shall—

(1) give notice of the existence and character of each existing system once a year to the Federal Privacy Board;

(2) give public notice of the existence and character of each existing system each year, in the case of Federal organizations in the Federal Register, or in the case of other organizations in local or regional printed media likely to bring attention to the existence of the records to data subjects;

(3) publish such annual notices for all its existing systems simultaneously;

(4) in the case of a new system, or the substantial modification of an existing system, shall give public notice and notice to the Federal Privacy Board within a reasonable time but in no case less than three months, in advance of the initiation or modification to assure individuals who may be affected by its operation a reasonable opportunity to comment; and

(5) assure that public notice given under this subsection specifies the following:

(A) the name of the system;

(B) the general purposes of the system;

(C) the categories of personal information and approximate number of persons on whom information is maintained;

(D) the categories of information maintained, confidentiality requirements, and access controls;

(E) the organization's policies and practices regarding information storage, duration of retention of information, and purging of such information;

(F) the categories of information sources;

(G) a description of types of use made of

cance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.

Government and private data collection on individuals is not a brand new phenomenon. The Federal Government has been collecting immense amounts of very sensitive information on individuals for decades. Income tax, social security, and census come to mind immediately. Various surveys by experts, private organizations such as the National Academy of Sciences, and a number of congressional committees have established the fact that the Federal Government stores massive amounts of information about all of us.

Nevertheless, the effect on the right to privacy of massive information-gathering and dissemination through the use of sophisticated computer technology is just beginning to be realized. Rich or poor, male or female, whatever one's cultural syle or religious or political views, each of us is the subject to cumulative records being stored by a variety of Government agencies and private organizations.

One of the most obvious threats the computer poses to privacy comes in its ability to collect, store, and disseminate information without any subjective concern for human emotion and fallability.

Yet the increasing growth of information-gathering by Government and private organizations proceeds without any standards or procedures to regulate these organizations. It is because of this vacuum of authority that I am introducing, along with the very distinguished ranking minority member, Senator PERCY, this bill which is essential in order to preserve individual freedoms. We must act now to create safeguards against the present and potential abuse of information about people. I would like to provide a brief summary of its provisions.

THE FEDERAL PRIVACY BOARD

The bill establishes a Federal Privacy Board which shall have the primary function of overseeing the gathering, maintenance and disclosure of information concerning individuals by Federal agencies, State and local governments, and private organizations.

This Federal Privacy Board consists of five members, appointed by the President with the advice and consent of the Senate, not more than three of which are to be of the same political party. No member may engage in any other employment during his tenure.

In addition to its primary responsibility in enforcing the safeguards to personal privacy proscribed under section II of this bill, the Board is responsible for making an annual report to the President and to Congress, as well as publishing, on an annual basis, a descriptive directly of all information systems currently operating in the United States.

In order to carry out its functions, the Board is designated several specific powers. First, the Board shall have the power to compel, through subpena if necessary, the production of any documents relating to an information system, either private or public.

Second, upon determination of a violation of any provisions of this act, the Board is authorized to issue cease and desist orders and to recommend the institution of either criminal or civil suits.

Third, the Board can conduct open, public hearings on any petition for exemption from the provisions of section II of the act. Upon completion of its hearings, the Board will report is recommendation to the Congress.

SAFEGUARDS FOR PERSONAL PRIVACY IN INFORMATION SYSTEMS

The bill provides safeguards to personal privacy at all three stages of the information systems process: collection, maintenance, and dissemination of information.

COLLECTION OF INFORMATION

Under the provisions of the bill, information may be gathered by Federal agencies, State and local governments, or any private organizations only to accomplish the proper purposes of those agencies and organizations.

In gathering information, the individual must be the source of that information to the greatest extent possible; however, no individual may be forced to disclose any information not required by law, and he is to be informed of his right not to disclose.

The individual is to be notified of the existence of any information being maintained on him and the uses to which that information is being put.

No public or private organization may collect information on an individual's political or religious beliefs or affiliations unless specified by law.

A description of all information systems must be reported to the Federal Privacy Board on an annual basis.

MAINTENANCE

Restrictions on the maintenance of information systems used by Federal agencies, State and local governments, and other organizations include requirements that all information in these systems be accurate, complete, timely, and pertinent.

Any individual has the right to inspect the information maintained in a system relating to him with the exception of medical records. He has the right to know the nature of the source and the recipients of that information.

The individual also has the right to challenge any information on the basis of its accuracy, completeness, timeliness, pertinence, or necessity. Upon receipt of any challenge to its information by an individual, an organization must: First, investigate and record the current status of such information; second, purge any information that is found to be incomplete, not pertinent, not timely, not necessary to be maintained, or that can no longer be verified.

If the investigation does not solve the dispute, the individual may insert a statement, not in excess of 200 words, in his own defense, and he may appeal to the Federal Privacy Board.

DISSEMINATION

The bill places strict restrictions on the dissemination of information in personal information systems, both private and public.

All information systems must request permission from the individual before disseminating any information to any person or organization not having regular, authorized access to the information system.

Organizations maintaining information systems are required to keep an accurate list of all persons having access to the information including but not limited to those having access on a regular basis.

Federal agencies are specifically restricted in disseminating information only to authorized employees of Federal agencies.

SOCIAL SECURITY NUMBERS

The Omnibus Privacy Bill makes it unlawful for any organization to require an individual to disclose or furnish his social security number unless specifically required by law.

MAILING LISTS

The bill also provides for the removal of any name and address from a mailing list upon the written request of the individual.

REMEDIES

The remedies provide under this act include both criminal and civil sanctions.

The act provides for a criminal liability of up to $10,000 or 5 years in prison, or both, for any violation of the act.

In addition, the act provides that the Attorney General, upon the recommendation of the Federal Privacy Board, or an aggrieved individual, may file a civil suit in the appropriate district court.

EXEMPTIONS

Certain types of information are exempted from coverage of this act. Those information systems exempted include: any information maintained by a Federal agency and determined to be vital to national defense; criminal investigatory files of Federal, State or local law enforcement agencies; and any information maintained by the press or news media—except that information related to the employees of such organizations.

CONCLUSION

Mr. President, this bill provides a method whereby the Congress can guarantee that the right of every American to be let alone will be maintained. I encourage every Senator to support this important piece of legislation.

I ask unanimous consent that the text of the bill be printed in the RECORD at this point.

There being no objection the text of the bill was ordered to be printed in the RECORD as follows:

S. 3418

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

other employers or which subjects the United States or its employees to a penalty or liability because of this section. An agency of the United States may not accept pay from a city for services performed in withholding city income or employment taxes from the pay of employees of the agency.

"(c) For the purpose of this section—

"(1) 'city' means a city which is duly incorporated under the laws of a State and within the political boundaries of which 500 or more persons are regularly employed by all agencies of the Federal Government; and

"(2) 'agency' means—

"(A) an Executive agency;

"(B) the judicial branch; and

"(C) the United States Postal Service."

(b) The analysis of subchapter II of chapter 55 of title 5, United States Code, is amended by adding at the end thereof—

"520. Withholding of city income or employment taxes.".

SEC. 2. Section 410(b) of titl 39, United States Code, is amended by striking out the words "and section 5532 (dual pay)" and inserting in lieu thereof "section 5520 (withholding city income or employment taxes), and section 5532 (dual pay)".

SEC. 3. This section shall become effective on the date of enactment of this Act. The provisions of the first section and section 2 of this Act shall become effective on the ninetieth day following the date of enactment.

By Mr. ERVIN (for himself, Mr. PERCY, and Mr. MUSKIE):

S. 3418. A bill to establish a Federal Privacy Board to oversee the gathering and disclosure of information concerning individuals, to provide management systems in Federal agencies, State and local governments, and other organizations regarding such information, and for other purposes. Referred to the Committee on Government Operations.

ESTABLISHMENT OF A FEDERAL PRIVACY BOARD

Mr. ERVIN. Mr. President, with the concurrence of Mr. PERCY and Mr. MUSKIE I introduce for reference to the Government Operations Committee a bill to establish a Federal Privacy Board, to oversee the gathering and disclosure of information concerning individuals, and to provide management systems in all Federal agencies, State and local governments, and other organizations.

Recent months have focused a great deal of attention, both in the Congress and with the public at large, on one of our most fundamental civil liberties—the right to privacy.

The Constitution creates a right to privacy which is designed to assure that the minds and hearts of Americans remain free. The bulwark of this constitutional principle is the first amendment. The first amendment was designed to protect the sanctity of the individual's private thoughts and beliefs. It protects the individual's right to free exercise of conscience; his right to assemble to petition the Government for redress of grievances; his right to associate peaceably with others of like mind in pursuit of a common goal; his right to speak freely what he believes; and his right to try to persuade others of the worth of his ideas.

The fourth amendment guarantees "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In addition to the privacy of one's home and personal effects, the privacy of his person—or bodily integrity—and even his private telephone conversations are protected by the fourth amendment. The fifth amendment guarantees that an individual shall not be forced to divulge private information which might incriminate him. It also protects individual privacy by preventing unwarranted governmental interference with the individual's person, personality, and property without due process of law.

The ninth amendment's reservation that "the enumeration in the Constitution of certain rights, shall not be construed to deny or disparage others retained by the people" clearly shows that the Founding Fathers contemplated that certain basic individual rights not specifically mentioned in the Constitution—such as privacy—should nevertheless be safe from governmental interference.

The Supreme Court has held many aspects of individual privacy to be constitutionally protected. In recognizing that "specific guarantees in the Bill of Rights have penumbras formed by emanations from those guarantees that help give them life and substance" (*Griswold* v. *Connecticut*, 381 U.S. 479, 484) the Court has found that those penumbras protect the right to give and receive information, the right to family life and child-rearing according to one's conscience, the right to marriage, the right to procreation, the right to contraception, and the right to abortion.

All Americans can testify to the power of those protections of the individual's rights. The Constitution assures these rights to all citizens whether their exercise is pleasing to Government or not. And by the same token, it assures the individual the converse of these rights: the right not to speak what he believes, whether his silence is pleasing to Government or not; and his right not to act, not to associate, not to assemble, whether his inaction is pleasing to Government or not.

The right of every individual in America to privacy has been a matter of considerable concern to me over the years. It seems that now, as never before, the appetite of government and private organizations for information about individuals threatens to usurp the right to privacy which I have long felt to be among the most basic of our civil liberties as a free people.

If we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens. Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.

Alexander Solzyhenitsyn, the Russian Nobel Prize winner, suggests how an all-knowing government dominates its citizens in his book "Cancer Ward:"

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions. . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber, banks, buses, trams and even people would all lose the ability to move, and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city. They are not visible, they are not material, but every man is constantly aware of their existence. . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.

Perhaps it should come as no surprise that a Russian can master the words to describe the elusive concept we in America call personal privacy. He understands, in a way which we cannot, the importance of being a free individual with certain inalienable rights, an individual secure in the knowledge that his thoughts and judgments are beyond the reach to the state or any man. He understands those concepts because he has no such security or rights but lives in a country where rights written into law are empty platitudes.

Privacy, like many of the other attributes of freedom, can be easiest appreciated when it no longer exists. A complacent citizenry only becomes outraged about its loss of integrity and individuality when the aggrandizement of power in the Government becomes excessive. By then, it may be too late. We should not have to conjure up 1984 or a Russian-style totalitarianism to justify protecting our liberties against Government encroachment. Nor should we wait until there is such a threat before we address this problem. Protecting against the loss of a little liberty is the best means of safeguarding ourselves against the loss of our freedom.

The protection of personal privacy is no easy task. It will require foresight and the ability to forecast the possible trends in information technology and the information policies of our Government and private organizations before they actually take their toll in widespread invasions of the personal privacy of large numbers of individual citizens. Congress must act before sophisticated new systems of information gathering and retention are developed, and before they produce widespread abuses. The peculiarity of new complex technologies is that once they go into operation, it is too late to correct our mistakes or supply our oversight.

Our Founding Fathers had that foresight when they wrote the Bill of Rights. The first, fourth and fifth amendments are among the most effective bulwarks to personal freedom conceived by the mind of man. Justice Brandeis in his classic dissent in the wiretapping case, *Olmstead* v. *United States*, 277 U.S. 438, 478 (1927), described with unsurpassed eloquence the importance of the right to privacy set out in the Constitution. These words do not go stale from repetition:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the signifi-